



# COPY

For : The Patent Application

Our Ref. : NT0226US

● LIST OF THE PRIOR ART REFERENCES CITED IN THE SPECIFICATION

1. Advances in Cryptology-CRYPTO etc.
2. The Chain & Sum Primitive and Its Applications to MACs  
And Stream Ciphers  
Mariusz H. Jakubowski and Ramarathnam Venkatesan  
(281-293)  
"Advances in Cryptology CRYPTO'98" Kaisa Nyberg (Ed.)
3. Keying Hash Functions for Message Authentication  
Mihir Bellare and Ran Canetti and Hugo Krawczyk (1-328)  
"Advances in Cryptology CRYPTO'96" Neal Koblitz (Ed.)
4. An Integrity Check Value Algorithm for Stream Ciphers  
Richard Taylor (40-48)  
"Advances in Cryptology CRYPTO'93" Douglas R. Stinson (Ed.)
5. Algorithm Types and Modes (189-401)
6. UMAC: Fast and Secure Message Authentication  
J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway  
(pg. 216-269)  
"Advances in Cryptology CRYPTO'99" Michael Wiener (Ed.)
7. MMH: Software Message Authentication in the Gbit/Second  
Rates Shai Halevi and Hugo Krawczyk (172-189)  
"Fast Software Encryption" Eli Biham (Ed.)

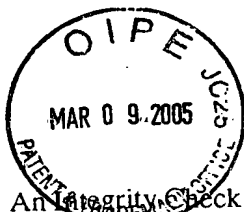
8. Integrity-Aware PCBC Encryption Schemes

Virgil D Gligor, Pompiliu Donescu (1-13)

"The 1999 Security Protocols Workshop Pre-proceedings"

9. Stream ciphers based on LFSRs (203-369)

## Reference



Richard Taylor	An Integrity Check Value Algorithm for Stream	pp.40-48	LNCS773	CRYPTO93
Mihir Bellare	Keying Hash Functions for Message Authentication	pp.1-15		CRYPTO96
Ran Canetti	Universal Hashing and Multiple Authentication	pp.16-30	LNCS1109	CRYPTO96
Hugo Krawczyk	Universal Hash Functions from Exponential Sums over Finite Fields and On Fast and Provably Secure Message Authentication Based on The Chain & Sum Primitive and Its Applications to MACs and Stream Ciphers	pp.31-44	LNCS1109	CRYPTO96
M. Atici		pp.313-328	LNCS1109	CRYPTO96
D. R. Stinson		pp.281-293	LNCS1403	EUROCRYPT98
Tor Helleseht	UMAC: Fast and Secure Message Authentication	pp.216-233	LNCS1666	CRYPTO99
Thomas Johansson	Square Hash: Fast Message Authentication via Optimized Universal Hash Constructing VIL-MACs from FIL-MACs: Message Authentication under Weakened Assumptions	pp.234-251	LNCS1666	CRYPTO99
Victor Shoup	MMH: Software Message Authentication in the Gbit/Second Rates	pp.252-269	LNCS1666	CRYPTO99
Mariusz H. Jakubowski		pp.172-189	LNCS1267	FSE97
Ramarathnam Venkatesan				
J Black				
S. Halevi				
H. Krawczyk				
T. Krovetz				
P. Rogaway				
Mark Etzel				
Sarvar Patel				
Zulfikar Ramzan				
Jee Hea An				
Mihir Bellare				
Shai Halevi				
Hugo Krawczyk				
Virgil D. Gligor	Integrity-Aware PCBC Encryption Schemes			The 1999 Security Protocols Workshop Pre-proceedings, Cambridge UK, 1999.
Pompiliu Donescu		pp.203-212, 250-259, 263-266, 347-349, 352-359, 363-366, 371-374, 377-380, 383-386, 389-392, 395-398, 399-402, 405-408, 411-414, 417-420, 423-426, 429-432, 435-438, 441-444, 447-450, 453-456, 459-462, 465-468, 471-474, 477-480, 483-486, 489-492, 495-498, 499-502, 505-508, 511-514, 517-520, 523-526, 529-532, 535-538, 541-544, 547-550, 553-556, 559-562, 565-568, 571-574, 577-580, 583-586, 589-592, 595-598, 599-602, 605-608, 611-614, 617-620, 623-626, 629-632, 635-638, 641-644, 647-650, 653-656, 659-662, 665-668, 671-674, 677-680, 683-686, 689-692, 695-698, 699-702, 705-708, 711-714, 717-720, 723-726, 729-732, 735-738, 741-744, 747-750, 753-756, 759-762, 765-768, 771-774, 777-780, 783-786, 789-792, 795-798, 799-802, 805-808, 811-814, 817-820, 823-826, 829-832, 835-838, 841-844, 847-850, 853-856, 859-862, 865-868, 871-874, 877-880, 883-886, 889-892, 895-898, 899-902, 905-908, 911-914, 917-920, 923-926, 929-932, 935-938, 941-944, 947-950, 953-956, 959-962, 965-968, 971-974, 977-980, 983-986, 989-992, 995-998, 999-1002, 1005-1008, 1011-1014, 1017-1020, 1023-1026, 1029-1032, 1035-1038, 1041-1044, 1047-1050, 1053-1056, 1059-1062, 1065-1068, 1071-1074, 1077-1080, 1083-1086, 1089-1092, 1095-1098, 1099-1102, 1105-1108, 1111-1114, 1117-1120, 1123-1126, 1129-1132, 1135-1138, 1141-1144, 1147-1150, 1153-1156, 1159-1162, 1165-1168, 1171-1174, 1177-1180, 1183-1186, 1189-1192, 1195-1198, 1199-1202, 1205-1208, 1211-1214, 1217-1220, 1223-1226, 1229-1232, 1235-1238, 1241-1244, 1247-1250, 1253-1256, 1259-1262, 1265-1268, 1271-1274, 1277-1280, 1283-1286, 1289-1292, 1295-1298, 1299-1302, 1305-1308, 1311-1314, 1317-1320, 1323-1326, 1329-1332, 1335-1338, 1341-1344, 1347-1350, 1353-1356, 1359-1362, 1365-1368, 1371-1374, 1377-1380, 1383-1386, 1389-1392, 1395-1398, 1399-1402, 1405-1408, 1411-1414, 1417-1420, 1423-1426, 1429-1432, 1435-1438, 1441-1444, 1447-1450, 1453-1456, 1459-1462, 1465-1468, 1471-1474, 1477-1480, 1483-1486, 1489-1492, 1495-1498, 1499-1502, 1505-1508, 1511-1514, 1517-1520, 1523-1526, 1529-1532, 1535-1538, 1541-1544, 1547-1550, 1553-1556, 1559-1562, 1565-1568, 1571-1574, 1577-1580, 1583-1586, 1589-1592, 1595-1598, 1599-1602, 1605-1608, 1611-1614, 1617-1620, 1623-1626, 1629-1632, 1635-1638, 1641-1644, 1647-1650, 1653-1656, 1659-1662, 1665-1668, 1671-1674, 1677-1680, 1683-1686, 1689-1692, 1695-1698, 1699-1702, 1705-1708, 1711-1714, 1717-1720, 1723-1726, 1729-1732, 1735-1738, 1741-1744, 1747-1750, 1753-1756, 1759-1762, 1765-1768, 1771-1774, 1777-1780, 1783-1786, 1789-1792, 1795-1798, 1799-1802, 1805-1808, 1811-1814, 1817-1820, 1823-1826, 1829-1832, 1835-1838, 1841-1844, 1847-1850, 1853-1856, 1859-1862, 1865-1868, 1871-1874, 1877-1880, 1883-1886, 1889-1892, 1895-1898, 1899-1902, 1905-1908, 1911-1914, 1917-1920, 1923-1926, 1929-1932, 1935-1938, 1941-1944, 1947-1950, 1953-1956, 1959-1962, 1965-1968, 1971-1974, 1977-1980, 1983-1986, 1989-1992, 1995-1998, 1999-2002, 2005-2008, 2011-2014, 2017-2020, 2023-2026, 2029-2032, 2035-2038, 2041-2044, 2047-2050, 2053-2056, 2059-2062, 2065-2068, 2071-2074, 2077-2080, 2083-2086, 2089-2092, 2095-2098, 2099-2102, 2105-2108, 2111-2114, 2117-2120, 2123-2126, 2129-2132, 2135-2138, 2141-2144, 2147-2150, 2153-2156, 2159-2162, 2165-2168, 2171-2174, 2177-2180, 2183-2186, 2189-2192, 2195-2198, 2199-2202, 2205-2208, 2211-2214, 2217-2220, 2223-2226, 2229-2232, 2235-2238, 2241-2244, 2247-2250, 2253-2256, 2259-2262, 2265-2268, 2271-2274, 2277-2280, 2283-2286, 2289-2292, 2295-2298, 2299-2302, 2305-2308, 2311-2314, 2317-2320, 2323-2326, 2329-2332, 2335-2338, 2341-2344, 2347-2350, 2353-2356, 2359-2362, 2365-2368, 2371-2374, 2377-2380, 2383-2386, 2389-2392, 2395-2398, 2399-2402, 2405-2408, 2411-2414, 2417-2420, 2423-2426, 2429-2432, 2435-2438, 2441-2444, 2447-2450, 2453-2456, 2459-2462, 2465-2468, 2471-2474, 2477-2480, 2483-2486, 2489-2492, 2495-2498, 2499-2502, 2505-2508, 2511-2514, 2517-2520, 2523-2526, 2529-2532, 2535-2538, 2541-2544, 2547-2550, 2553-2556, 2559-2562, 2565-2568, 2571-2574, 2577-2580, 2583-2586, 2589-2592, 2595-2598, 2599-2602, 2605-2608, 2611-2614, 2617-2620, 2623-2626, 2629-2632, 2635-2638, 2641-2644, 2647-2650, 2653-2656, 2659-2662, 2665-2668, 2671-2674, 2677-2680, 2683-2686, 2689-2692, 2695-2698, 2699-2702, 2705-2708, 2711-2714, 2717-2720, 2723-2726, 2729-2732, 2735-2738, 2741-2744, 2747-2750, 2753-2756, 2759-2762, 2765-2768, 2771-2774, 2777-2780, 2783-2786, 2789-2792, 2795-2798, 2799-2802, 2805-2808, 2811-2814, 2817-2820, 2823-2826, 2829-2832, 2835-2838, 2841-2844, 2847-2850, 2853-2856, 2859-2862, 2865-2868, 2871-2874, 2877-2880, 2883-2886, 2889-2892, 2895-2898, 2899-2902, 2905-2908, 2911-2914, 2917-2920, 2923-2926, 2929-2932, 2935-2938, 2941-2944, 2947-2950, 2953-2956, 2959-2962, 2965-2968, 2971-2974, 2977-2980, 2983-2986, 2989-2992, 2995-2998, 2999-3002, 3005-3008, 3011-3014, 3017-3020, 3023-3026, 3029-3032, 3035-3038, 3041-3044, 3047-3050, 3053-3056, 3059-3062, 3065-3068, 3071-3074, 3077-3080, 3083-3086, 3089-3092, 3095-3098, 3099-3102, 3105-3108, 3111-3114, 3117-3120, 3123-3126, 3129-3132, 3135-3138, 3141-3144, 3147-3150, 3153-3156, 3159-3162, 3165-3168, 3171-3174, 3177-3180, 3183-3186, 3189-3192, 3195-3198, 3199-3202, 3205-3208, 3211-3214, 3217-3220, 3223-3226, 3229-3232, 3235-3238, 3241-3244, 3247-3250, 3253-3256, 3259-3262, 3265-3268, 3271-3274, 3277-3280, 3283-3286, 3289-3292, 3295-3298, 3299-3302, 3305-3308, 3311-3314, 3317-3320, 3323-3326, 3329-3332, 3335-3338, 3341-3344, 3347-3350, 3353-3356, 3359-3362, 3365-3368, 3371-3374, 3377-3380, 3383-3386, 3389-3392, 3395-3398, 3399-3402, 3405-3408, 3411-3414, 3417-3420, 3423-3426, 3429-3432, 3435-3438, 3441-3444, 3447-3450, 3453-3456, 3459-3462, 3465-3468, 3471-3474, 3477-3480, 3483-3486, 3489-3492, 3495-3498, 3499-3502, 3505-3508, 3511-3514, 3517-3520, 3523-3526, 3529-3532, 3535-3538, 3541-3544, 3547-3550, 3553-3556, 3559-3562, 3565-3568, 3571-3574, 3577-3580, 3583-3586, 3589-3592, 3595-3598, 3599-3602, 3605-3608, 3611-3614, 3617-3620, 3623-3626, 3629-3632, 3635-3638, 3641-3644, 3647-3650, 3653-3656, 3659-3662, 3665-3668, 3671-3674, 3677-3680, 3683-3686, 3689-3692, 3695-3698, 3699-3702, 3705-3708, 3711-3714, 3717-3720, 3723-3726, 3729-3732, 3735-3738, 3741-3744, 3747-3750, 3753-3756, 3759-3762, 3765-3768, 3771-3774, 3777-3780, 3783-3786, 3789-3792, 3795-3798, 3799-3802, 3805-3808, 3811-3814, 3817-3820, 3823-3826, 3829-3832, 3835-3838, 3841-3844, 3847-3850, 3853-3856, 3859-3862, 3865-3868, 3871-3874, 3877-3880, 3883-3886, 3889-3892, 3895-3898, 3899-3902, 3905-3908, 3911-3914, 3917-3920, 3923-3926, 3929-3932, 3935-3938, 3941-3944, 3947-3950, 3953-3956, 3959-3962, 3965-3968, 3971-3974, 3977-3980, 3983-3986, 3989-3992, 3995-3998, 3999-4002, 4005-4008, 4011-4014, 4017-4020, 4023-4026, 4029-4032, 4035-4038, 4041-4044, 4047-4050, 4053-4056, 4059-4062, 4065-4068, 4071-4074, 4077-4080, 4083-4086, 4089-4092, 4095-4098, 4099-4102, 4105-4108, 4111-4114, 4117-4120, 4123-4126, 4129-4132, 4135-4138, 4141-4144, 4147-4150, 4153-4156, 4159-4162, 4165-4168, 4171-4174, 4177-4180, 4183-4186, 4189-4192, 4195-4198, 4199-4202, 4205-4208, 4211-4214, 4217-4220, 4223-4226, 4229-4232, 4235-4238, 4241-4244, 4247-4250, 4253-4256, 4259-4262, 4265-4268, 4271-4274, 4277-4280, 4283-4286, 4289-4292, 4295-4298, 4299-4302, 4305-4308, 4311-4314, 4317-4320, 4323-4326, 4329-4332, 4335-4338, 4341-4344, 4347-4350, 4353-4356, 4359-4362, 4365-4368, 4371-4374, 4377-4380, 4383-4386, 4389-4392, 4395-4398, 4399-4402, 4405-4408, 4411-4414, 4417-4420, 4423-4426, 4429-4432, 4435-4438, 4441-4444, 4447-4450, 4453-4456, 4459-4462, 4465-4468, 4471-4474, 4477-4480, 4483-4486, 4489-4492, 4495-4498, 4499-4502, 4505-4508, 4511-4514, 4517-4520, 4523-4526, 4529-4532, 4535-4538, 4541-4544, 4547-4550, 4553-4556, 4559-4562, 4565-4568, 4571-4574, 4577-4580, 4583-4586, 4589-4592, 4595-4598, 4599-4602, 4605-4608, 4611-4614, 4617-4620, 4623-4626, 4629-4632, 4635-4638, 4641-4644, 4647-4650, 4653-4656, 4659-4662, 4665-4668, 4671-4674, 4677-4680, 4683-4686, 4689-4692, 4695-4698, 4699-4702, 4705-4708, 4711-4714, 4717-4720, 4723-4726, 4729-4732, 4735-4738, 4741-4744, 4747-4750, 4753-4756, 4759-4762, 4765-4768, 4771-4774, 4777-4780, 4783-4786, 4789-4792, 4795-4798, 4799-4802, 4805-4808, 4811-4814, 4817-4820, 4823-4826, 4829-4832, 4835-4838, 4841-4844, 4847-4850, 4853-4856, 4859-4862, 4865-4868, 4871-4874, 4877-4880, 4883-4886, 4889-4892, 4895-4898, 4899-4902, 4905-4908, 4911-4914, 4917-4920, 4923-4926, 4929-4932, 4935-4938, 4941-4944, 4947-4950, 4953-4956, 4959-4962, 4965-4968, 4971-4974, 4977-4980, 4983-4986, 4989-4992, 4995-4998, 4999-5002, 5005-5008, 5011-5014, 5017-5020, 5023-5026, 5029-5032, 5035-5038, 5041-5044, 5047-5050, 5053-5056, 5059-5062, 5065-5068, 5071-5074, 5077-5080, 5083-5086, 5089-5092, 5095-5098, 5099-5102, 5105-5108, 5111-5114, 5117-5120, 5123-5126, 5129-5132, 5135-5138, 5141-5144, 5147-5150, 5153-5156, 5159-5162, 5165-5168, 5171-5174, 5177-5180, 5183-5186, 5189-5192, 5195-5198, 5199-5202, 5205-5208, 5211-5214, 5217-5220, 5223-5226, 5229-5232, 5235-5238, 5241-5244, 5247-5250, 5253-5256, 5259-5262, 5265-5268, 5271-5274, 5277-5280, 5283-5286, 5289-5292, 5295-5298, 5299-5302, 5305-5308, 5311-5314, 5317-5320, 5323-5326, 5329-5332, 5335-5338, 5341-5344, 5347-5350, 5353-5356, 5359-5362, 5365-5368, 5371-5374, 5377-5380, 5383-5386, 5389-5392, 5395-5398, 5399-5402, 5405-5408, 5411-5414, 5417-5420, 5423-5426, 5429-5432, 5435-5438, 5441-5444, 5447-5450, 5453-5456, 5459-5462, 5465-5468, 5471-5474, 5477-5480, 5483-5486, 5489-5492, 5495-5498, 5499-5502, 5505-5508, 5511-5514, 5517-5520, 5523-5526, 5529-5532, 5535-5538, 5541-5544, 5547-5550, 5553-5556, 5559-5562, 5565-5568, 5571-5574, 5577-5580, 5583-5586, 5589-5592, 5595-5598, 5599-5602, 5605-5608, 5611-5614, 5617-5620, 5623-5626, 5629-5632, 5635-5638, 5641-5644, 5647-5650, 5653-5656, 5659-5662, 5665-5668, 5671-5674, 5677-5680, 5683-5686, 5689-5692, 5695-5698, 5699-5702, 5705-5708, 5711-5714, 5717-5720, 5723-5726, 5729-5732, 5735-5738, 5741-5744, 5747-5750, 5753-5756, 5759-5762, 5765-5768, 5771-5774, 5777-5780, 5783-5786, 5789-5792, 5795-5798, 5799-5802, 5805-5808, 5811-5814, 5817-5820, 5823-5826, 5829-5832, 5835-5838, 5841-5844, 5847-5850, 5853-5856, 5859-5862, 5865-5868, 5871-5874, 5877-5880, 5883-5886, 5889-5892, 5895-5898, 5899-5902, 5905-5908, 5911-5914, 5917-5920, 5923-5926, 5929-5932, 5935-5938, 5941-5944, 5947-5950, 5953-5956, 5959-5962, 5965-5968, 5971-5974, 5977-5980, 5983-5986, 5989-5992, 5995-5998, 5999-6002, 6005-6008, 6011-6014, 6017-6020, 6023-6026, 6029-6032, 6035-6038, 6041-6044, 6047-6050, 6053-6056, 6059-6062, 6065-6068, 6071-6074, 6077-6080, 6083-6086, 6089-6092, 6095-6098, 6099-6102, 6105-6108, 6111-6114, 6117-6120, 6123-6126, 6129-6132, 6135-6138, 6141-6144, 6147-6150, 6153-6156, 6159-6162, 6165-6168, 6171-6174, 6177-6180, 6183-6186, 6189-6192, 6195-6198, 6199-6202, 6205-6208, 6211-6214, 6217-6220, 6223-6226, 6229-6232, 6235-6238, 6241-6244, 6247-6250, 6253-6256, 6259-6262, 6265-6268, 6271-6274, 6277-6280, 6283-6286, 6289-6292, 6295-6298, 6299-6302, 6305-6308, 6311-6314, 6317-6320, 6323-6326, 6329-6332, 6335-6338, 6341-6344, 6347-6350, 6353-6356, 6359-6362, 6365-6368, 6371-6374, 6377-6380, 6383-6386, 6389-6392, 6395-6398, 6399-6402, 6405-6		